Ростелеком
Солар

Новые реалии: аналитика, кейсы и рекомендации от Solar JSOC

Денис Баскаков
Директор ЕЦК «Восток» Ростелеком-Солар

Ситуация сегодня

90% компаний, находящихся под защитой «Ростелеком-Солар» от DDoS-атак, ежедневно подвергаются нападениям **широковещательным DDoS с использованием преимущественно заграничных ботнетов**

DDoS-атаки – своего рода дымовая завеса. Неприятно, но не смертельно

Массовые атаки на веб-ресурсы: **дефейс через взлом счетчиков и баннеров**. Это несет репутационный урон, но прямого взлома сайтов и утечек персональных данных с государственных ресурсов не происходит

Необратимое **шифрование** данных **без возможности выкупа**

За атаками в основном стоят **APT- и проправительственные группировки**. Но и менее квалифицированные злоумышленники не дремлют.

Проправительственные группировки повысили активность в части **проникновения и закрепления в объектах КИИ и компаниях госсектора на территории РФ**

Громкие заголовки со словом «кибератака» – в большинстве случаев лишь **манипуляция фактами и акт запугивания**

Успешных кибератак с реальным ущербом среди клиентов Solar JSOC **на текущий момент не выявлено**

Ростелеком Солар

Динамика за февраль/март 2022 года

Рост числа всех типов атак по отраслям (активные заражения инфраструктур)

+4,7%	+10,6%	+15,4%	+16,2%	+16,5%	+18,8%	+22%
Образование	Телеком	Здравоохранение	ТЭК	Финансы	Промышленность	Госсектор

+14,9% Средний показатель роста атак

Ростелеком Солар

Динамика по СФО за март/май 2022г.

Рост числа всех типов атак по отраслям (активные заражения инфраструктур)

-5%	-4%	-8%	-11%	-9%	-7%	-10,5%
Образование	Телеком	Здравоохранение	ТЭК	Финансы	Промышленность	Госсектор

-12,3%

Пищепром

-8%

Средний показатель роста атак

Ростелеком Солар

Ключевые факторы последних лет

01

Переход на удаленную работу в связи с **пандемией** стал **тренировочной площадкой для обкатки новых решений** и **стимулом для вектора на повышение защищенности** в информационном пространстве

02

Формирование **приоритета на выполнение госзаказов в России** – один из элементов **цифровизации экономики**

03

Результаты быстрого развития ИТ:

- **«сырое» ПО** на рынке
- появление **новых рисков и угроз**

04

Следствие мирового экономического кризиса:

- **стагнация рынка**
- **рост цен** на конечные продукты

Ростелеком Солар

В каком состоянии ИТ-рынок вошел в 2022 год

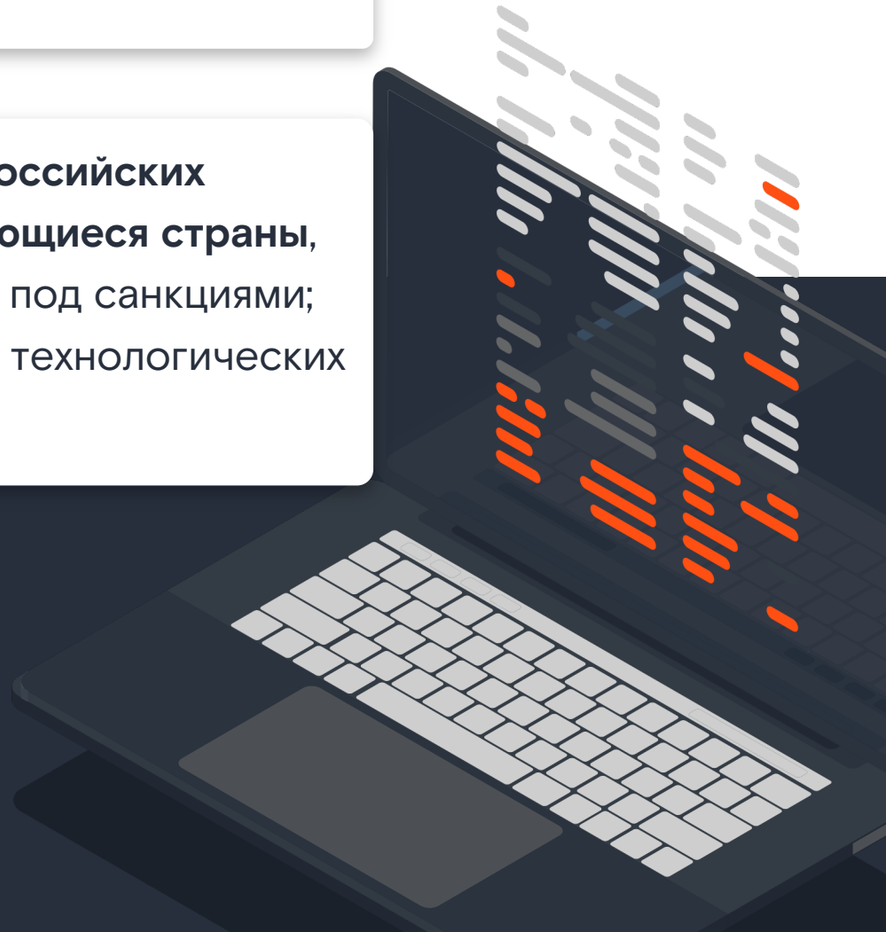
Рост российского рынка ИБ, увеличение бюджетирования данной сферы

Рост технологической защищенности различных секторов экономики, включая государственные организации

Развитие ИТ-инфраструктуры как важнейшего обеспечивающего элемента бизнеса, позволяющего сформировать целостную экосистему, способную противостоять новым угрозам

Налаживание **экспорта российских ИТ-продуктов в развивающиеся страны**, в том числе находящиеся под санкциями; развитие новых векторов технологических партнерств

Осознанная **цифровизация бизнеса с возросшими** за последние два года **темпами**



Уровни злоумышленников

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
Массовые атаки	Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
Массовые атаки	Киберхулиган/ Энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
Массовые атаки	Киберкриминал/ Организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, социнжиниринг
Профессиональные атаки	Кибернаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
Профессиональные атаки	Кибервойска/ Проправительственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные «закладки»

Ростелеком Солар

Чего ждать и к чему готовиться?

Атаки будут усложняться: киберпреступники будут использовать нетипичные методы и техники

Под прицелом в первую очередь окажутся **государственные органы и субъекты КИИ**

SMB по-прежнему остается сферой интересов **злоумышленников 3-го уровня**, основная цель которых - **монетизация**

Продолжится рост **атак через подрядчиков**

Продолжится **рост числа атак** со стороны **проправительственных группировок** на фоне «процветания» промышленного шпионажа

Атаки **проправительственных группировок** не всегда сразу будут вести к убыткам. Основным признаком деятельности киберпреступников 5-го уровня останется длительное присутствие

Продолжатся **атаки с использованием шифровальщиков для распространения паники**

Ростелеком Солар

Рекомендации

Контроль периметра

1. Регулярное проведение инвентаризации внешнего периметра
2. Отключение неиспользуемых сервисов
3. Использование решений для мониторинга внутреннего и внешнего периметра и открытых источников

Контроль внутренней инфраструктуры

1. Защита от сетевых угроз
2. Защита почты от спама, фишинга, шифровальщиков, вредоносного ПО
3. Организация регулярного аудита доменных групп

Веб-приложения

1. Круглосуточный мониторинг инцидентов
2. Защита публичных сервисов на всех уровнях сетевой модели OSI
3. Проверка веб-приложений на предмет наличия компонентов, загружаемых с внешних ресурсов

Ростелеком Солар

Сервисы

Контроль периметра

1. Защита от сетевых угроз (UTM)
2. Контроль уязвимостей (VM)
3. Анализ защищенности
4. Тестирование на проникновение
5. Анализ угроз и внешней обстановки (OSINT)

Контроль внутренней инфраструктуры

1. Мониторинг и реагирование на инциденты в режиме 24*7 (SOC)
2. Защита конечных точек от сложных кибератак (EDR)
3. Анализ сетевого трафика (NTA)
4. Управление процессами реагирования на инциденты (IRP)
5. Защита электронной почты (SEG)
6. Сервис защиты от продвинутых угроз (Sandbox)
7. Консалтинг в области процессов реагирования на инциденты

Веб-приложения

1. Защита от DDoS-атак (Anti-DDoS)
2. Защита веб-приложений (WAF)
3. Контроль и анализ уязвимостей с рекомендациями по их устранению

Защита пользователей

1. Защита электронной почты (SEG)
2. Управление навыками кибербезопасности (SA)
3. Сервис защиты от продвинутых угроз (Sandbox)

Ростелеком Солар

Solar JSOC

Первый и крупнейший в России коммерческий **центр противодействия кибератакам,** действующий по модели MDR (Managed Detection and Response). Обеспечивает защиту крупных государственных и коммерческих организаций от киберугроз и оказывает помощь другим корпоративным SOC.

Предотвращение

Разведка и раннее предупреждение об угрозах, оценка рисков и управление уязвимостями

Выявление

Расширенные возможности мониторинга и анализа событий кибербезопасности 24/7, противодействие атакам на ранней стадии

Реагирование

Оперативное техническое расследование, ликвидация последствий и устранение причин возникновения инцидентов

Построение SOC и консалтинг

Помощь в создании и совершенствовании центров управления кибербезопасностью

№1
на рынке SOC в России

400+
экспертов по кибербезопасности

250+
клиентов из всех отраслей экономики

110+
млрд анализируемых событий в сутки

10 минут
на обнаружение кибератаки

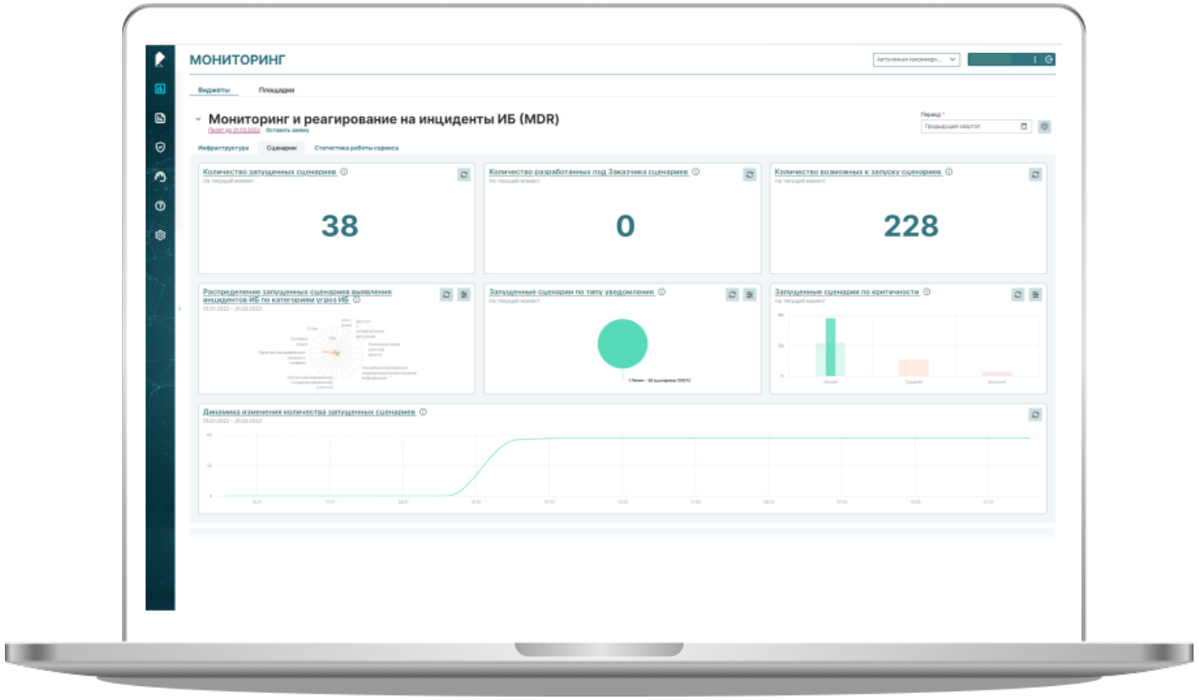
30 минут
на реагирование и защиту

Ростелеком Солар

Solar JSOC: что нового

Личный кабинет

- интуитивно понятный интерфейс
- системы оповещений и управления тикетами
- наглядные отчеты о работе сервисов и состоянии подключенной к мониторингу инфраструктуре



Ростелеком Солар

Ответы на вопросы

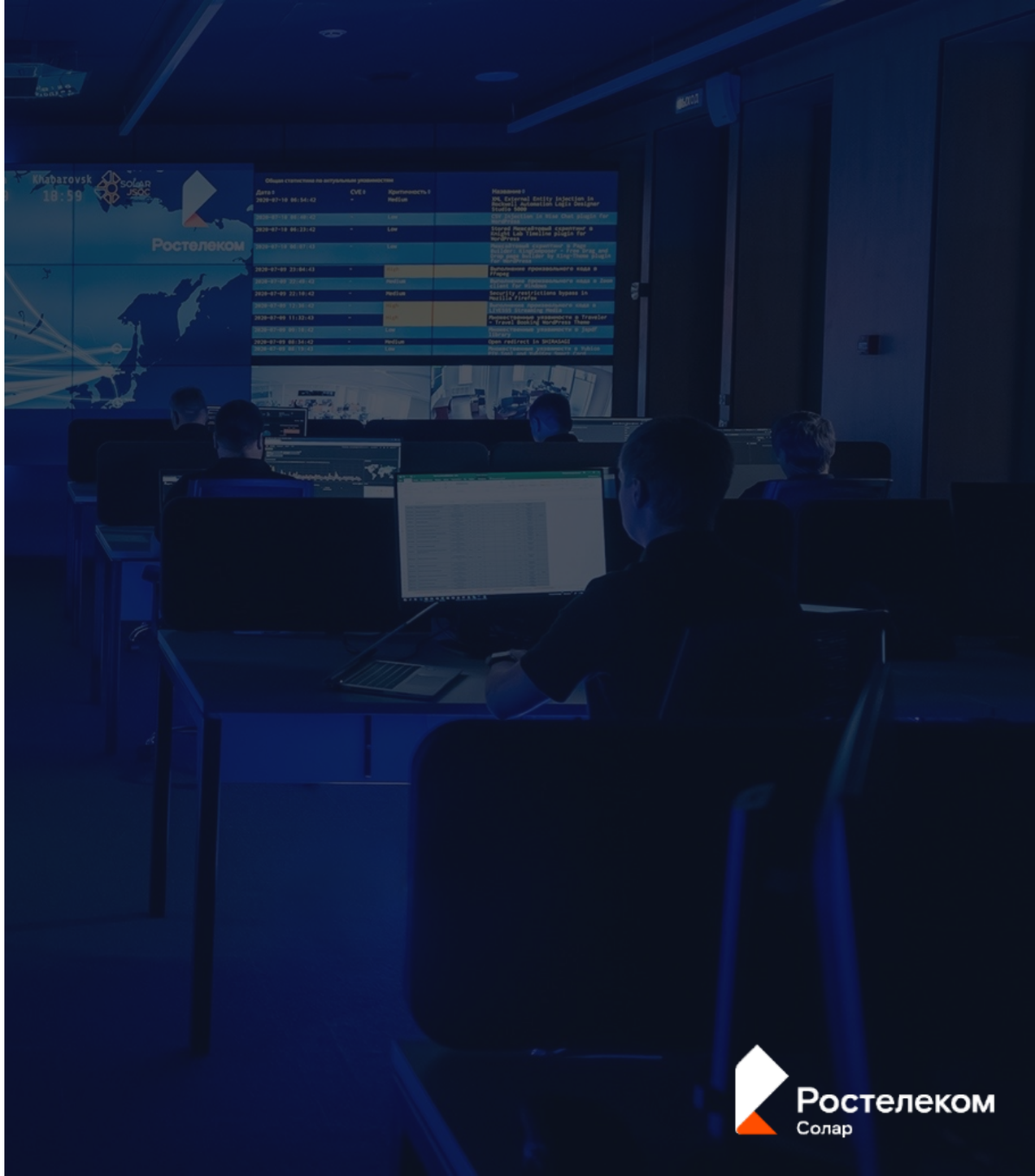
Денис Баскаков,

Директор ЕЦК «Восток» Ростелеком-Солар

Контакты

+7 (914) 707-67-87

d.baskakov@rt-solar.ru



Ростелеком
Солар